CLAIMS

1. A denial-of-service attack protecting method of protecting a communication device against a denial of service attack using a gate device or a repeater device, the gate device interposing between the repeater device that forms part of a network and the communication device that is a target of the denial of service attack, comprising:

an issuing step, in which an authorized device on the network issues authorized address information indicating a source address of a non-attacking packet; and

a restricting step, in which the gate device restricts passage of a packet that may attack on the communication device, based on the authorized address information issued by the authorized device.

2. The denial-of-service attack protecting method of protecting a communication device against a denial of service attack using a gate device or a repeater device, the gate device interposing between the repeater device that forms part of a network and the communication device that is a target of the denial of service attack, according to claim 1, further comprising:

an authorized address information acquiring step, in which the gate device acquires the authorized address information indicating a source address of a non-attacking packet transmitted by an authorized device on the network;

a normal condition information generating step, in which the gate device generates normal condition information indicating conditions for the non-attacking packet, based on the authorized address information acquired in the authorized address information acquiring step; and

a packet restricting step, in which the gate device restricts the passage of a packet that may attack on the communication device, while allowing the passage of a packet that matches the conditions indicated in the normal condition information generated in the normal condition information generating step, among packets received from the network.

3. The denial-of-service attack protecting method according to claim 2, wherein the authorized address information acquiring step includes

an address information reporting step, in which the gate device reports address information for its own device to the repeater device,

an authorized address information repeating step, in which, when receiving authorized address information from the authorized device, the repeater device repeats the authorized address information to the gate device based on the address information reported in the address information reporting step, and

a receiving step, in which the gate device receives the authorized address information.

4. The denial-of-service attack protecting method according to claim 3, wherein

in the address information reporting step, the repeater device, to which the address information for the gate device is reported, repeats the address information for the gate device to another repeater device that is provided adjacent to the repeater device, and

in the authorized address information repeating step, when receiving authorized address information from the authorized device, the another repeater device repeats the

authorized address information to an adjacent repeater device or the gate device based on the address information for the gate device.

5. The denial-of-service attack protecting method according to claim 2, wherein the authorized address information acquiring step includes

an authorized address information storing step, in which an authorized address information providing device, which integrally manages authorized address information, receives the authorized address information from each authorized device, and stores it,

an authorized address information reporting step, in which, when accepting a transmission request for the authorized address information from the gate device, the authorized address information providing device reports the authorized address information requested for its transmission, to the gate device, and

a receiving step, in which the gate device receives the authorized address information.

6. The denial-of-service attack protecting method according to any one of claims 2 to 5, wherein in the authorized address information acquiring step,

the gate device acquires the authorized address information transmitted by an address issuing device that issues an address or by a communication device that is authorized.

7. The denial-of-service attack protecting method according to claim 2, further comprising:

an attack detecting step, in which the gate device detects an attack performed by a packet received from the

network;

a suspicious signature generating step, in which the gate device generates a suspicious signature indicating a feature of the packet as one that has attacked, which is detected in the attack detecting step;

a normal condition information storing step, in which the gate device stores the normal condition information generated in the normal condition information generating step, in a normal condition information storage unit; and

a normal signature generating step, in which the gate device generates a normal signature indicating a feature of a packet, which matches conditions indicated in the normal condition information, among packets applying to the suspicious signature generated in the suspicious signature generating step, wherein

in the packet restricting step, the gate device restricts the passage of a packet received from the network based on the suspicious signature generated in the suspicious signature generating step and the normal signature generated in the normal signature generating step.

8. The denial-of-service attack protecting method according to claim 7, further comprising:

a signature reporting step, in which the gate device reports the suspicious signature generated in the suspicious signature generating step and the normal signature generated in the normal signature generating step, to the repeater device; and

a packet restriction controlling step, in which the repeater device controls restriction to the passage of a packet based on the suspicious signature and the normal signature reported in the signature reporting step.

9. The denial-of-service attack protecting method of protecting a communication device against a denial of service attack using a gate device or a repeater device, the gate device interposing between the repeater device that forms part of a network and the communication device that is a target of the denial of service attack, according to claim 1, further comprising:

an attack detecting step, in which the gate device detects an attack performed by a packet received from the network;

an authorized address information acquiring step, in which, when an attack on the communication device is detected in the attack detecting step, the gate device acquires authorized address information from the repeater device, the authorized address information indicating a source address of a non-attacking packet which is received from an authorized device on the network; and

a passage controlling step, in which the gate device controls the passage of a packet based on the normal condition information, indicating conditions for the non-attacking packet, which is generated from the authorized address information received from the repeater device.

10. The denial-of-service attack protecting method according to claim 9, further comprising:

a suspicious signature generating step, in which the gate device generates a suspicious signature indicating a feature of the packet as one that has attacked, which is detected in the attack detecting step, wherein in the authorized address information acquiring step,

the gate device transmits the suspicious signature generated in the suspicious signature generating step to the repeater device, and acquires authorized address

information sent back in response to the transmission.

11. The denial-of-service attack protecting method according to claim 10, wherein the passage controlling step includes

a normal condition information generating step of generating normal condition information indicating conditions for a non-attacking packet based on the authorized address information acquired in the authorized address information acquiring step, and

a packet restricting step of restricting the passage of a packet that may attack on the communication device, while allowing the passage of a packet that matches the conditions indicated in the normal condition information generated in the normal condition information generating step, among packets received from the network.

12. The denial-of-service attack protecting method according to claim 11, further comprising:

a normal signature generating step of generating a normal signature indicating a feature of a packet that matches conditions indicated in the normal condition information generated in the normal condition information generating step, wherein in the packet restricting step,

the passage of a packet received from the network is restricted based on the suspicious signature generated in the suspicious signature generating step and the normal signature generated in the normal signature generating step.

13. The denial-of-service attack protecting method according to claim 12, further comprising:

a signature forwarding step, in which the gate device forwards the normal signature generated in the normal

signature generating step, to the repeater device.

14. A denial-of-service attack protecting system for protecting a communication device against a denial of service attack using a gate device or a repeater device, the gate device interposing between the repeater device that forms part of a network and the communication device that is a target of the denial of service attack, wherein the gate device comprises:

an authorized address information acquiring unit that acquires authorized address information indicating a source address of a non-attacking packet transmitted by an authorized device on the network;

a normal condition information generating unit that generates normal condition information indicating conditions for the non-attacking packet, based on the authorized address information acquired by the authorized address information acquiring unit; and

a packet restricting unit that restricts the passage of a packet that may attack on the communication device, while allowing the passage of a packet that matches the conditions indicated in the normal condition information generated by the normal condition information generating unit, among packets received from the network.

15. A denial-of-service attack protecting system of protecting a communication device against a denial of service attack using a gate device or a repeater device, the gate device interposing between the repeater device that forms part of a network and the communication device that is a target of the denial of service attack, wherein the gate device comprising:

an attack detecting unit that detects an attack

performed by a packet received from the network;

an authorized address information acquiring unit that, when an attack on the communication device is detected by the attack detecting unit, acquires authorized address information from the repeater device, the authorized address information indicating a source address of a non-attacking packet which is received from an authorized device on the network; and

a passage controlling unit that controls the passage of a packet based on the normal condition information, indicating conditions for the non-attacking packet, which is generated from the authorized address information received from the repeater device.

16. A gate device that protects a communication device against a denial of service attack, the gate device interposing between a repeater device that forms part of a network and the communication device that is a target of the denial of service attack, comprising:

an attack detecting unit that detects an attack performed by a packet received from the network;

an authorized address information acquiring unit that, when an attack on the communication device is detected by the attack detecting unit, acquires authorized address information from the repeater device, the authorized address information indicating a source address of a non-attacking packet which is received from an authorized device on the network; and

a passage controlling unit that controls the passage of a packet based on the normal condition information, indicating conditions for the non-attacking packet, which is generated from the authorized address information received from the repeater device.

17. The gate device according to claim 16, wherein the authorized address information acquiring unit includes

an address information reporting unit that reports address information for its own device to the repeater device, and

a receiving unit that receives the authorized address information from the authorized device sent back by the repeater device in response to the address information for the own device reported by the address information reporting unit.

18. The gate device according to claim 17, wherein the authorized address information acquiring unit includes

an authorized address information transmission requesting unit that issues a transmission request for the authorized address information to an authorized address information providing device that integrally manages authorized address information, and

a receiving unit that receives the authorized address information sent back in response to the transmission request for the authorized address information.

19. A gate device that protects a communication device against a denial of service attack, the gate device interposing between a repeater device that forms part of a network and the communication device that is a target of the denial of service attack, comprising:

an attack detecting unit that detects an attack performed by a packet received from the network;

an authorized address information acquiring unit that, when an attack on the communication device is detected by the attack detecting unit, acquires authorized address

information from the repeater device, the authorized address information indicating a source address of a non-attacking packet which is received from an authorized device on the network; and

a passage controlling unit that controls the passage of a packet based on the normal condition information, indicating conditions for the non-attacking packet, which is generated from the authorized address information received from the repeater device.

20. The gate device according to claim 19, further comprising:

a suspicious signature generating unit that generates a suspicious signature indicating a feature of the packet as one that has attacked, which is detected by the attack detecting unit, wherein

the authorized address information acquiring unit transmits the suspicious signature generated by the suspicious signature generating unit to the repeater device, and acquires authorized address information sent back in response to the transmission.

21. The gate device according to claim 20, wherein the passage controlling unit includes

a normal condition information generating unit that generates normal condition information indicating conditions for a non-attacking packet based on the authorized address information acquired by the authorized address information acquiring unit, and

a packet restricting unit that restricts the passage of a packet that may attack on the communication device, while allowing the passage of a packet that matches the conditions indicated in the normal condition information

generated by the normal condition information generating unit, among packets received from the network.

22. A repeater device connected to a gate device that protects a communication device being a target of a denial of service attack, and/or connected to one or more repeater devices that form a network, comprising:

an address information acquiring unit that acquires address information for the gate device; and

an authorized address information repeating unit that repeats authorized address information to the gate device or another adjacent repeater device based on the address information acquired by the address information acquiring unit, when receiving the authorized address information indicating a source address of a non-attacking packet transmitted by an authorized device on the network.

23. A repeater device connected to a gate device that protects a communication device being a target of a denial of service attack, and/or connected to one or more repeater devices that form a network, comprising:

an authorized address information storage unit that stores authorized address information indicating a source address of a non-attacking packet received from an authorized device on the network; and

a transfer unit that transfers the authorized address information stored in the authorized address information storage unit when the gate device detects an attack on the communication device.

24. A computer program that causes a gate device to protect a communication device against a denial of service attack, the gate device interposing between a repeater

device that forms part of a network and the communication device that is a target of the denial of service attack, the computer program causing the gate device to execute:

an attack detecting step of detecting an attack performed by a packet received from the network;

an authorized address information acquiring of acquiring, when an attack on the communication device is detected in the attack detecting step, authorized address information from the repeater device, the authorized address information indicating a source address of a non-attacking packet which is received from an authorized device on the network; and

a passage controlling step of controlling the passage of a packet based on the normal condition information, indicating conditions for the non-attacking packet, which is generated from the authorized address information received from the repeater device.

25. The computer program according to claim 24, wherein the authorized address information acquiring step includes

an address information reporting step of reporting address information for its own device to the repeater device, and

a receiving step of receiving the authorized address information from the authorized device sent back by the repeater device in response to the address information for the own device reported at the address information reporting step.

26. The computer program according to claim 24, wherein the authorized address information acquiring step includes

an authorized address information transmission requesting step of issuing a transmission request for the

authorized address information to an authorized address information providing device that integrally manages authorized address information, and

a receiving step of receiving the authorized address information sent back in response to the transmission request for the authorized address information.

27. A computer program that causes a gate device to protect a communication device against a denial of service attack, the gate device interposing between a repeater device that forms part of a network and the communication device that is a target of the denial of service attack, the computer program causing the gate device to execute:

an attack detecting step of detecting an attack performed by a packet received from the network;

an authorized address information acquiring step of acquiring, when an attack is detected in the attack detecting step, authorized address information from the repeater device, the authorized address information indicating a source address of a non-attacking packet which is received from an authorized device on the network; and

a passage controlling step of controlling the passage of a packet based on the normal condition information, indicating conditions for the non-attacking packet, which is generated from the authorized address information received from the repeater device.

28. The computer program according to claim 27, wherein the computer program further causes the gate device to execute a suspicious signature generating step of generating a suspicious signature indicating a feature of the packet as one that has attacked, which is detected by the attack detecting unit, wherein

the authorized address information acquiring step includes transmitting the suspicious signature generated at the suspicious signature generating step to the repeater device, and acquires authorized address information sent back in response to the transmission.

29. The computer program according to claim 28, wherein the passage controlling step includes

a normal condition information generating step of generating normal condition information indicating conditions for a non-attacking packet based on the authorized address information acquired in the authorized address information acquiring step, and

a packet restricting step of restricting the passage of a packet that may attack on the communication device, while allowing the passage of a packet that matches the conditions indicated in the normal condition information generated in the normal condition information generating step, among packets received from the network.

30. A computer program that causes a repeater device connected to a gate device to protect a communication device being a target of a denial of service attack, and/or connected to one or more repeater devices that form a network, the computer program causing the repeater device to execute:

an address information acquiring step of acquiring address information for the gate device; and

an authorized address information repeating step of repeating authorized address information to the gate device or another adjacent repeater device based on the address information acquired at the address information acquiring step, when receiving the authorized address information

indicating a source address of a non-attacking packet transmitted by an authorized device on the network.

31. A computer program that causes a repeater device connected to a gate device to protect a communication device being a target of a denial of service attack, and/or connected to one or more repeater devices that form a network, the computer program causing the repeater device to execute:

an authorized address information storage step of storing authorized address information indicating a source address of a non-attacking packet received from an authorized device on the network; and

a transfer step of transferring authorized address information stored at the authorized address information storage step when the gate device detects an attack on the communication device.